CLAIMS

1. (previously presented) A unitary portable biometrics-based access control device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to a restricted resource, the device comprising:

a housing;

a microprocessor housed within the housing;

a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable access control device directly to the USB socket; and

a biometrics-based authentication module coupled to and controlled by the microprocessor, at least a portion of the biometrics-based authentication module being housed within the housing, wherein access to the restricted resource is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the restricted resource is denied to the user otherwise.

2. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module is a fingerprint authentication module.

3. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module is an iris scan authentication module.

4. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the housing.

5. (previously presented) The portable device as recited in Claim 1 further comprising a non-volatile memory capable of storing biometrics information usable for authentication.

6. (previously presented) The portable device as recited in Claim 1 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

7. (previously presented) The portable device as recited in Claim 1 wherein the restricted resource comprises a host computer.

8. (previously presented) The portable device as recited in Claim 1 wherein the restricted resource comprises a communication network.

9. (previously presented) The portable device as recited in Claim 1 wherein the restricted resource is a real estate premises that imposes access restrictions.

10. (previously presented) The portable device as recited in Claim 1 wherein the restricted resource is an operable machinery, the safe operation of which requires training.

11. (previously presented) A biometrics-based access control system for controlling access to a restricted resource, comprising:

a portable device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to the restricted resource and which includes a housing; a non-volatile memory housed within the housing; a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device directly to the USB socket; and a biometrics-based authentication module coupled to the non-volatile memory, wherein the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker, and wherein access to the restricted resource is granted upon a determination of successful authentication and wherein access to the restricted resource is denied otherwise.

12. (previously presented) The biometrics-based access control system as recited in Claim 11 wherein the biometrics-based authentication module is a fingerprint authentication module.

13. (previously presented) The biometrics-based access control system as recited in Claim 11 wherein the biometrics-based authentication module is an iris scan authentication module.

14. (previously presented) The biometrics-based access control system as recited in Claim 11 wherein the biometrics-based authentication module comprises a biometrics sensor which is structurally integrated with the portable device in a unitary construction, the biometrics sensor being disposed on one surface of the housing of the portable device.

15. (previously presented) The biometrics-based access control system as recited in Claim 11 wherein the non-volatile memory of the portable device comprises flash memory.

16. (previously presented) The biometrics-based access control system as recited in Claim 11 wherein a bypass mechanism for authentication is provided upon a determination of authentication failure by the biometrics-based authentication module.

17. (previously presented) A biometrics-based access control method for controlling access to a restricted resource and implemented using a portable device, the method comprising the steps of:

(a) directly plugging the portable device into a universal serial bus (USB) socket communicatively coupled to the restricted resource, wherein the portable device includes a housing; a memory; a biometrics sensor; and a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device directly to the USB socket;

(b) obtaining a first biometrics marker from a user with the biometrics sensor of the portable device;

(c) retrieving a registered biometrics marker from the memory of the portable device, the registered biometrics marker having been stored therein during a registration process;

(d) comparing the first biometrics marker against the registered biometrics marker; and

(e) granting the user access to the restricted resource provided that a match is identified in said step (d).

18. (previously presented) The biometrics-based access control method as recited in Claim 17 wherein the registered biometrics marker is a fingerprint.

19. (previously presented) The biometrics-based access control method as recited in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.

20. (previously presented) The biometrics-based access control method as recited in Claim 17 further comprising the step of denying the user access to the restricted resource provided that a match is not identified in said step (d).

21. (previously presented) The biometrics-based access control method as recited in Claim 17 further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (d).